IN THE CLAIMS

Please amend the claims as follows:

1. - 33. (Canceled)

34. (NEW) A border server comprising:

secure connection software for secure communication with a client where the client resides in an insecure network;

insecure connection software for communicating with a target server where the target server resides in a secure network; and

a transformer to transform a secure request received from the client to an insecure request for the target server, and the transformer also transforms insecure data received from the target server into secure data while the client is authenticated and then sends the secure data to the client computer.

35. (NEW) The border server of claim 34, wherein the transformer transforms the secure request, which is a Uniform Resource Locator (URL) request, and wherein the secure connection software is used by a browser of the client to issue the secure request.

36. (NEW) The border server of claim 34, wherein the transformer transforms the insecure data by sending the insecure data to the client as the secure data using a Hypertext Markup Transfer Protocol over a Secure Sockets Layer (HTTPS) which is used by the secure connection software.

37. (NEW) The border server of claim 34, wherein the target server is indirectly accessible to the client via the transformer while the client remains authenticated.

38. (NEW) The border server of claim 34, wherein the client is authenticated by an authentication system on the secure network.

39. (NEW) The border server of claim 34, wherein the transformer maintains a cache having the secure data for servicing subsequent requests for the secure data.

40. (NEW) The border server of claim 34 further comprising a redirector that intercepts and redirects the secure requests to the transformer.

41. (NEW) A method for operating a border server, said method comprising:

receiving a secure request from a client over an insecure network;

transforming the secure request into an insecure request while authenticating the client and sending the insecure request to a target server residing in a secure network;

receiving insecure data from the target server; and

transforming the insecure data into secure data and sending the secure data to the client over the insecure network, if the client was successfully authenticated.

42. (NEW) The method of claim 41 further comprising checking a cache within the secure network for the insecure data before sending the insecure request to the target server.

43. (NEW) The method of claim 41 wherein the receiving further includes intercepting, by the border server, the secure request sent from the client, wherein the secure request was originally directed from the client to the target server.

44. (NEW) The method of claim 41 wherein the transforming of the secure request further includes sending the insecure request to the target server within a secure intranet environment which is the secure network.

45. (NEW) The method of claim 41 wherein the transforming of the secure request includes using a directory services database in connection with an authentication system to authenticate the client.

46. (NEW) The method of claim 41 wherein the transforming of the secure request includes blocking, by the border server, direct access from the client to the target server.

47. (NEW) The method of claim 41 wherein the receiving further includes receiving a username and password with the secure request which is used when authenticating the client.

48. (NEW) A method for operating a border server, comprising:

intercepting a secure request issued from a client for secure data accessible from a secure network, wherein the secure request is intercepted from an insecure network;

authenticating the client while transforming the secure request into an insecure request within the secure network; and

locating the secure data within the secure network and transforming the secure data into insecure data for delivery to the client over the insecure network using secure communications.

49. (NEW) The method of claim 48 wherein the intercepting further includes intercepting the secure request that was originally directed to a target server having the secure data and located within the secure network.

50. (NEW) The method of claim 48 wherein the locating further includes using Secure Socket Layer protocols as the secure communications over the Internet which is the insecure network.

51. (NEW) The method of claim 48 wherein the locating further includes issuing the insecure request to a target server within the secure network in order to acquire the secure data.

52. (NEW) The method of claim 48 wherein the locating further includes checking a cache for the secure data.

53. (NEW) The method of claim 48 further comprising, storing the secure data in a cache accessible from the secure network to satisfy subsequent secure requests for the secure data.